09/694,416 : Reexam 2131

HDP/SB/21 based on PTO/SB/21 (08-00)

~~90/005776~~

OIPE MAY 0 9 2005 PATENT & TRADEMARK OFFICE

Please type a plus sign (+) inside this box → +

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	~~09/964,416~~
Filing Date	October 20, 2000
Inventor(s)	Thomas COLLINS et al.
Group Art Unit	2131
Examiner Name	James Seal
Attorney Docket Number	6215-000124/RED

ENCLOSURES *(check all that apply)*

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [x] Supplemental Amendment
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
- [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Assignment Papers *(for an Application)*
- [ ] Letter to the Official Draftsperson and _____ Sheets of Formal Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance Communication to Group
- [ ] LETTER SUBMITTING APPEAL BRIEF AND APPEAL BRIEF (w/clean version of pending claims)
- [ ] Appeal Communication to Group *(Notice of Appeal, Brief, Reply Brief)*
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) *(please identify below)*:

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Harness, Dickey & Pierce, P.L.C.	Attorney Name John A. Castellano	Reg. No. 35,094
Signature			
Date	May 9, 2005		

PATENT
HD_6215-000124/RED

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Reissue App. No.: 09/694,416	**Related to:**
Patent No. 5,848,159	**Re-Examination Control No. 90/005,733 and**
Issued: 12/8/1998	**Re-Examination Control No. 90/005,776** ✓

Filing Date:	October 20, 2000		
Applicant:	Thomas Collins et al.		
Examiner:	James Seal	Group Art Unit:	2131
Title:	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD		
Attorney Docket:	200301647-5		

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

May 9, 2005

SUPPLEMENTAL AMENDMENT

Sir:

In response to the communication mailed April 8, 2005, the following response is respectfully submitted in connection with the above-identified application.

Amendments to the Claims begin on page 2 of this Amendment.

Remarks begin on page 28 of this Amendment.

IN THE CLAIMS

1. (Twice Amended) A method for [[establishing cryptographic]] communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption, comprising the [[step]] steps of:

developing k distinct random prime numbers $p_1, p_2, \ldots, p_k$, wherein k is an integer greater than 2;

providing a number e relatively prime to $(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)$;

providing a composite number n equaling the product $p_1 \cdot p_2 \cdot \ldots \cdot p_k$;

receiving a ciphertext word signal C which is formed by encoding a plaintext message word signal M to a ciphertext word signal C, where M corresponds to a number representative of [[a]] the message and

$0 \leq M \leq n-1$,

[[n being a composite number formed from the product of $p_1 \cdot p_2 \ldots \cdot p_k$ where k is an integer greater than 2, p_1, p_2, . . . p_k are distinct prime numbers, and]] where C is a number representative of an encoded form of the plaintext message word signal M such that $C \equiv M^e \pmod{n}$, and where e is associated with an intended recipient of the ciphertext word signal C; and [[, wherein said encoding step comprises the step of: transforming said message word signal M to said ciphertext word signal C whereby

$C=M^e \pmod{n}$

where e is a number relatively prime to $(p_1 -1) \cdot (p_2 -1)$]]

deciphering the received ciphertext word signal C at the intended recipient having available to it the k distinct random prime number $p_1, p_2, \ldots p_k$.

2. (Twice Amended)The method according to claim 1, [[comprising the further step of:]] wherein the deciphering step includes

establishing a number, d, as a multiplicative inverse of e(mod(lcm((p_1 -1), (p_2 -1), ..., (p_k -1)))), and

decoding the ciphertext word signal C to the plaintext message word signal M[[, wherein said decoding step comprises the step of: transforming said ciphertext word signal C]] where[[by:]] [[M=C^d (mod n)]] M≡C^d (mod n).

[[where d is a multiplicative inverse of e(mod(lcm((p_1 -1), (p_2 -1), . . . , (p_k - 1)))).]]

3. (Twice Amended) A method for [[transferring a message signal M_i in a]] communications of a message signal M_i cryptographically processed with RSA public key encryption in a system having j terminals, [[wherein]] each terminal [[is]] being characterized by an encoding key E_i =(e_i, n_i) and a decoding key D_i=(d_i, n_i), where i=1, 2, ... , j, and [[wherein]] the message signal M_i corresponds to a number representative of a message-to-be-received [[transmitted]] from the i^{th} terminal, the method comprising the steps of:

establishing n_i where n_i is a composite number of the form

[[$n_i = P_{i,1} \cdot p_{i,2} \cdot , \ldots , \cdot p_{i,k}$]] $n_i = p_{i,1} \cdot p_{i,2} \cdot , \ldots , \cdot p_{i,k}$

where k is an integer greater than 2,

$p_{i,1}$, $p_{i,2}$, . . . , $p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to [[lcm($p_{i,1}$ -1, $p_{1,2}$ -1, $p_{i,k}$ -1)]] lcm($p_{i,1}$ -1, $p_{i,2}$ -1,... $p_{i,k}$ -1), and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_i (mod(lcm(($p_{i,1}$ -1), ($p_{i,2}$ -1), . . . , ($p_{i,k}$ -1))));[[, comprising the step of:]]

receiving by a recipient terminal (i = y) from a sender terminal (i = x, x ≠ y) a

ciphertext signal C_X formed by encoding a digital message word signal M_x, wherein the encoding includes [[M_A for transmission from a first terminal (i=A) to a second terminal (i=B), said encoding step including the sub-step of:]]

transforming said message word signal M_A to one or more message block word signals [[M_A"]] M_X", each block word signal [[M_A"]] M_X" corresponding to a

number representative of a portion of said message word signal [[M_A]] $\underline{M_X}$ in the range $\underline{0 \leq M_X'' \leq n_y - 1}$ [[$0 \leq M_A'' \leq n_B - 1$]], and

transforming each of said message block word signals [[M_A'']] $\underline{M_X''}$ to a ciphertext word signal [[C_A, C_A corresponding]] $\underline{C_X}$ that corresponds to a number representative of an encoded form of said message block word signal [[M_A'']] $\underline{M_X''}$ [[,]] where[[by:]] [[$C_A \equiv M_A^{\,\prime\prime eB} \pmod{n_B}$]] $\underline{C_x \equiv M_x^{\,\prime\prime ey} \pmod{n_y}}$; and

deciphering the received ciphertext word signal C_x at the recipient terminal having available to it the k distinct random prime numbers $p_{y,1}, p_{y,2}, \ldots, p_{y,k}$ for establishing its d_y.

4. (Four Times Amended) A [[cryptographic communications]] system for communications of a message cryptographically processed with an RSA public key encryption, comprising:
a communication [[medium]] channel for transmitting a ciphertext word signal C;
[[an]] encoding means coupled to said channel and adapted for transforming a transmit message

word signal M to [[a]] the ciphertext word signal C using a composite number, n, where n is a product of the form

$n = p_1 \cdot p_2 \cdots p_k$

k is an integer greater than 2, and

$p_1, p_2, \ldots p_k$ are distinct random prime numbers [[and for transmitting C on said channel]], where the transmit message word signal M corresponds to a number representative of [[a]] the message and

$0 \leq M \leq n-1$ [[where n is a composite number of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

where k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and]]

where the ciphertext word signal C corresponds to a number representative of an [[enciphered]] encoded form of said message through a relationship of the form [[and corresponds to]]

$C \equiv M^e \pmod{n}$, and

where e is a number relatively prime to $\operatorname{lcm}(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$; and

[[a]] decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and, having available to it the k distinct random prime numbers $p_1, p_2, \ldots p_k$, for transforming the ciphertext word signal C to a receive

message word signal M' where M' corresponds to a number representative of a [[deciphered]] decoded form of the ciphertext word signal C [[and corresponds to]] through a relationship of the form $M' \equiv C_d$ (mod n)

where d is selected from the group consisting of [[the]] a class of numbers equivalent to a multiplicative inverse of

$e(\mathrm{mod}(\mathrm{lcm}((p_1 -1), (p_2 -1),\ldots,(p_k -1))))$.

5. (Twice Amended) A [[cryptographic communications]] system for communications of a message cryptographically processed with an RSA public key encryption, the system having a plurality of terminals coupled by a communications channel, [[including]] comprising:

a first terminal of the plurality of terminals characterized by an [[associated]] encoding key $E_A = (e_A, n_A)$ and a decoding key $D_A = (d_A, n_A)$,

where[[in]] n_A is a composite number of the form

$n_A = p_{A,1} \cdot p_{A,2} \cdot \ldots \cdot p_{A,k}$

where

k is an integer greater than 2,

$p_{A,1}, p_{A,2}, \ldots, p_{A,k}$ are distinct random prime numbers,

e_A is relatively prime to

$\mathrm{lcm}(p_{A,1} -1, p_{A,2} -1, \ldots, p_{A,k} -1)$, and

d_A is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_A (\mathrm{mod}(\mathrm{lcm}((p_{A,1} -1), (p_{A,2} -1), \ldots, (p_{A,k} -1))))$; and[[,]]

[[and including]] a second terminal of the plurality of terminals having[[, comprising:]]

blocking means for transforming a first message,[[-to-be-transmitted]] which is to be transmitted on said communications channel from said second terminal to said first terminal, into one or more transmit message word signals M_B, where each M_B corresponds to a number representative of said first message in the range

$0 \leq M_B \leq n_A - 1$,

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that [[and for transmitting C_B on said channel, where C_B]] corresponds to a number representative of an [[enciphered]] encoded form of said first message [[and corresponds to]] through a relationship of the form

[[$C_B \equiv M_B^{eA} \pmod{n_A}$]] $C_B \equiv M_B^{eA} \pmod{n_A}$,

[[wherein]] said first terminal having [[comprises:]]

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_B from said channel and, having available to it the k distinct

random prime numbers $p_{A,1}, p_{A,2}, \ldots p_{A,k}$, for transforming each of said ciphertext word signals C_B to a receive message word signal [[M_B]] M'_B, and

means for transforming said receive message word signal[[s]] [[M']] M'_B to said first message, where [[M']] M'_B [[is]] corresponds to a number representative of a [[deciphered]] decoded form of C_B [[and corresponds to]] through a relationship of the form

[[$M'_B \equiv C_B^{dA} \pmod{n_A}$]] $M'_B \equiv C_B^{dA} \pmod{n_A}$.

6. (Twice Amended) The system according to claim 5 wherein said second terminal is characterized by an [[associated]] encoding key [[$E_B = (e_B, n_B)$]] $E_B = (e_B, n_B)$ and a decoding key [[$DB = (D_B, d_B)$]] $D_B = (d_B, n_B)$, where[[:]]

n_B is a composite number of the form

$n_B = p_{B,1}$ [[$\cdot$]]$p_{B,2} \cdot \ldots \cdot p_{B,k}$

where k is an integer greater than 2,

$p_{B,1}, p_{B,2}, \ldots, p_{B,k}$ [[$P_{B,1}, P_{B,2}, \ldots, P_{B,k}$]] are distinct prime numbers,

e_B is relatively prime to

$lcm(p_{B,1} - 1, p_{B,2} - 1, \ldots, p_{B,k} - 1)$, and

d_B is selected from the group consisting of [[the]] a class of numbers equivalent to a multiplicative inverse of

e_B (mod(lcm(($p_{B,1}$-1), ($p_{B,2}$ -1), . . . , ($p_{B,k}$ -1)))),

[[wherein]] said first terminal [[comprises:]] further having

blocking means for transforming a second message, [[to-be-transmitted] which is to be transmitted on said communications channel from said first terminal to said second terminal, to one or more transmit message word signals M_A, where each M_A corresponds to a number representative of said message in the range [[$0 \leq M_A^{eB}$ (mod n_B)]] $0 \leq M_A \leq n_B - 1$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, [[

]] where C_A corresponds to a number representative of an encoded [[enciphered]] form of said second message [[and corresponds to]] through a relationship of the form

[[$C_A \equiv M_A^{eB}$ (mod n_B)]] $C_A \equiv M_A^{eB}$ (mod n_B)

[[wherein]] said second terminal [[comprises;]] further having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_A from said channel and, having available to it the k distinct random prime numbers $p_{B,1}, p_{B,2}, \ldots p_{B,k}$, for transforming each of said ciphertext word signals to a receive message word signal [[M_A ']] M'_A, and

means for transforming said receive message word signals [[M_A]] $\underline{M'_A}$ to said second message, [[

]] where [[M']] $\underline{M'_A}$ corresponds to a number representative of a [[deciphered]] decoded form of C_A [[and corresponds to]] through a relationship of the form [[$M_A{}' \equiv C_A^{dB} \pmod{n_B}$]] $\underline{M'_A \equiv C_A^{dB} \pmod{n_B}}$.

7. Cancel claim 7.

8. Cancel claim 8.

9. (Twice Amended) A [[communication]] system for [[transferring]] communications of message signals [[M_i]] cryptographically processed with RSA public key encryption, comprising:

j terminals including first and second terminals [[stations]], each of the j [[stations]] terminals being characterized by an encoding key $E_i=(e_i, n_i)$ and decoding key $D_i=(d_i, n_i)$[[ ]], where i=1,2, . . . ,j, [[and wherein

M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal,]] each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is transmitted from an i^{th} terminal and

$0 \leq M_i \leq n_i - 1$,

n_i [[is]] being a composite number of the form

[[$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$]] $\underline{n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to

$\mathrm{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots, p_{i,k}-1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a

multiplicative inverse of

$e_i\ (\mathrm{mod}(\mathrm{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))))$;

said [[a]] first terminal [[one of the j terminals]] including

means for encoding a digital message word signal [[M_A]] M_1 [[for transmission]] to be transmitted from said first terminal (i=1[[A]]) to [[a]] said second terminal [[one of the j terminals]] (i=2[[B]]), said encoding means [[for]] transforming said digital message word signal [[M_A]] M_1 to a signed message word signal [[M_{As}]] M_{1s} using a relationship of the form

[[, M_{1s} corresponding to a number representative of an encoded form of said message word signal M_A,

whereby:]]

[[$M_{AS} \equiv M_A^{dA} \pmod{n_A}$]] $M_{1s} \equiv M_1^{d1} \pmod{n_1}$; and

means for transmitting said signed message word signal M_{1s} from said first terminal to said second terminal, wherein said second terminal includes

means for decoding said message word signal M_{1s}' to said digital message word signal M_1.

10. (Twice Amended) The system of claim 9 [[further comprising:

means for transmitting said signal message word signal M_{As} from said first

terminal to said second terminal, and wherein said second terminal includes means for decoding said signed message word signal M_{As} to said digital message word signal M_A, said second terminal including:

means for]] wherein the decoding signed message word signal M_{As} includes means for transforming from said signed message word signal M_{As} [[, whereby]] using a relationship of the form

[[$M_A \equiv M_{As}^{eA} \pmod{n_A}$]] $M_1 \equiv M_{1s}^{e1} \pmod{n_1}$.

11. (Twice Amended) A communications system for transferring a message signal [[M_i]] cryptographically processed with RSA public key encryption, the communications system comprising:

j communication stations including first and second stations, each of the j communication stations being characterized by an encoding key $E_i=(e_i, n_i)$ and a decoding key $D_i=(d_i, n_i)$, where $i=1, 2, \ldots, j$, [[and wherein M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal,]] each of the j communication stations being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is received from an i^{th} communication station, and

$0 \le M_i \le n_1 - 1$

n_i [[is]] being a composite number of the form

$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\mathrm{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots, p_{i,k}-1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_i (mod(lcm(($p_{i,1}$ -1), ($p_{i,2}$ -1), . . . , ($p_{i,k}$ -1)))),

said first station [[one of the j communication stations]] including

means for encoding a digital message word signal [[M_A]] M_1 [[for transmission]] to be transmitted from said first station [[one of the j communication stations]] (i=1[[A]]) to [[a]] said second station [[one of the j communication stations]] (i=2[[B]]),

means for transforming said digital message word signal [[M_A]] M_1 to one or more message block word signals [[M_A ']] M_1", each block word signal [[M_A ']] M_1" being a number representative of a portion of said message word signal [[M_A ']] M_1 in the range

$0 \leq M_1" \leq n_2 - 1$ [[$0 \leq M_A \leq n_B - 1$]], and

means for transforming each of said message block word signals M_1" [[M_A]] to a ciphertext word signal C1 using a relationship of the form [[C_A, C_A corresponding to a number representative of an encoded form of said message block word signal M_A ", whereby :]]

[[$C_A \equiv M_A"^{Eb}$ (mod n_B)]] $C_1 \equiv M"_1{}^{e2}$ (mod n_2); and

means for transmitting said ciphertext signals C_1 from said first station to said second station, wherein said second station includes

means for deciphering said ciphertext signals C_1 using $p_{2,1}$, $p_{2,2}$, ... $p_{2,k}$ to produce said message word signal M_1.

12. (Twice Amended) The communications system of claim 11, [[further comprising: means for transmitting said ciphertext word signals from said first terminal to said second terminal, and]] wherein [[said second terminal]] the deciphering means includes

means for decoding said ciphertext word signals C_1 to said message block word signals [[MA]] M_1" using a relationship of the form [[, said second terminal including:

means for transforming each of said ciphertext word signals C_A to one of said message block word signals M_A", whereby

M_A "$\equiv C_A^{Db}$ (mod n_B)]] $M"_1 \equiv C_1^{d2}$ (mod n_2), and

means for transforming said message block word signals [[M_A"]] M_1 " to said message word signal [[M_A]] M_1.

13. Cancel claim 13.

14. (Previously Presented) A method of communicating a message cryptographically processed with an RSA public key encryption, comprising the steps of:

selecting a public key portion e associated with a recipient intended for receiving the message;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k_i distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message formed by encoding a plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e$ (mod n), where M represents the message, where $0 \leq M \leq n-1$ and where the sender knows n and the public key portion e but has no access to the k distinct random prime numbers, $p_1, p_2, \ldots p_k$; and

deciphering at the recipient the received ciphertext message data C to produce the message, the recipient having access to the k distinct random prime numbers, $p_1, p_2, \ldots p_k$.

15. (Previously Presented) The method according to claim 14, comprising the further step of:

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1 -1)\cdot(p_2 -1)\cdots(p_k -1)))$,

wherein the deciphering step includes decoding the ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

16. (Previously Presented) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} (\mathrm{mod}((p_1-1)\cdot(p_2 -1)\cdots(p_k -1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message data C representing an encoded form of a plaintext message data M; and

decoding the received ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$, the decoding performed by a recipient owning the private key portion d and having access to the k distinct random prime numbers, $p_1, p_2, \ldots p_k$.

17. (Previously Presented) The method according to claim 16, wherein the ciphertext message data C is formed by encoding the plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, wherein $0 \leq M \leq n-1$ and wherein n and the public key portion e are accessible to the sender although it has no access to the k distinct random prime numbers, $p_1, p_2, \ldots p_k$.

18. (Previously Presented) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1} (\text{mod}((p_1 -1)\cdot(p_2 -1)\cdots(p_k -1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers;

encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d$ (mod n), where $0 \leq M \leq n-1$

receiving the signed message M_s; and

deciphering the signed message to produce the plaintext message data M.

19. (Previously Presented) The method of claim 18, wherein the deciphering step includes:

decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e$ (mod n).

20. (Previously Presented) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

sending to a recipient a cryptographically processed message formed by assigning a number M to represent the message in plaintext message form, and

cryptographically transforming the assigned number M from the plaintext message form to a number C that represents the message in an encoded form, wherein the number C is a function of

the assigned number M,

a number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e having been obtained by the sender are associated with the recipient to which the message is intended; and

receiving the cryptographically processed message which is decipherable by the recipient based on

the number n,

another exponent d, and

the number C,

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers.

21. (Previously Presented) The method according to claim 20,

wherein the cryptographically transforming step includes using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent d is established based on the at least three distinct random prime numbers, $p_1, p_2, \cdots p_k$, using a relationship of the form $d \equiv e^{-1} (\bmod((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$, and

wherein the cryptographically processed message is deciphered using a relationship of the form $M \equiv C^d \pmod{n}$.

22. (Previously Presented) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

receiving from a sender a cryptographically processed message, in the form of a number C, which is decipherable by the recipient based on a number n, an exponent d, and the number C; and

deciphering the cryptographically processed message,

wherein a number M represents a plaintext form of the message, wherein the number C represents a cryptographically encoded form of the message and is a function of the number M,

the number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e are associated with the recipient to which the message is intended, and

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers.

23. (Previously Presented) The method according to claim 22,
wherein the number C is formed using a relationship of the form $C \equiv M^e \pmod{n}$,
wherein the exponent d is established based on the at lest three distinct random prime numbers, $p_1, p_2, \ldots p_k$, using a relationship of the form $d \equiv e^{-1} (\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,
and wherein the number M is obtained using a relationship of the form $M \equiv C^d \pmod{n}$.

24. (Previously Presented) The method according to claim 21,
wherein p and q are a pair of prime numbers the product of which equals n,
wherein the deciphering the number C to derive the number M is divided into subtasks, one subtask for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q,
whereby for a given length of n it takes fewer computational cycles to perform the deciphering relative to the number of computational cycles for performing such deciphering if the pair of prime numbers p and q were instead.

25. (Previously Presented) The method according to claim 22,
wherein p and q are a pair of prime numbers the product of which equals n,
wherein the deciphering the number C to derive the number M is divided into subtasks, one subtask for each of the k distinct random prime numbers,
wherein k distinct random prime numbers are each smaller than p and q,
whereby for a give length of n it takes fewer computational cycles to perform the deciphering relative to the number of computational cycles for performing such deciphering if the pair of prime numbers p and q were used instead.

26. (Previously Presented) The method according to claim 20,
wherein p and q are a pair of prime numbers the product of which equals n, and wherein developing the at least three distinct random prime numbers and computing n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

27. (Previously Presented) The method according to claim 22,
wherein p and q are a pair of prime numbers the product of which equals n, and
wherein developing the at least three distinct random prime numbers and computing n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

28. (Previously Presented) The method according to claim 14,
wherein p and q are a pair of prime numbers the product of which equals n,
wherein the deciphering step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller that p and q,
whereby for a given length of n it takes fewer computational cycles to perform the deciphering step relative to the number of computational cycles for performing such deciphering step if the pair of prime numbers p and q were used instead.

29. (Previously Presented) The method according to claim 14,
wherein p and q are a pair of prime numbers the product of which equals n, and
wherein developing the k distinct random prime numbers and computing the composite number n are performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

30. (Previously Presented) The method according to claim 16,
wherein p and q are a pair of prime numbers the product of which equals n,
wherein the decoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q,
whereby for a given length of n it takes fewer computational cycles to perform the decoding step relative to the number of computational cycles for performing such decoding step if the pair of prime numbers p and q were used instead.

31. (Previously Presented) The method according to claim 16,
wherein p and q are a pair of prime numbers the product of which equals n, and

wherein developing the k distinct random prime number and computing the composite n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

32. (Previously Presented) The method according to claim 18,
wherein p and q are a pair of prime numbers the product of which equals n,
wherein the encoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q,
whereby for a given length of n it takes fewer computational cycles to perform the encoding step relative to the number of computational cycles for performing such encoding step if the pair of prime numbers p and q were used instead.

33. (Previously Presented) The method according to claim 18,
wherein p and q are a pair of prime numbers that product of which equals n, and
wherein developing the k distinct random prime numbers and computing the composite number n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

34. (Previously Presented) The method according to claim 14, wherein a message cryptographically processed by the sender with two-rime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable with multi-prime (k>2) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, $p_1, p_2, \ldots p_k$.

35. (Three Times Amended) The method according to claim 9, wherein the signed message word signal M_{1s}, formed from the digital message word signal M_1 being cryptographically processed at the first terminal with multi-prime (k>2) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, $p_1, p_2, \ldots p_k$, is decipherable at the second terminal

with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q.

36. (Previously Presented) The method according to claim 16, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable by the decoding with multi-prime (k>2) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, $p_1, p_2, \ldots p_k$.

37. (Previously Presented) The method according to claim 18, wherein the signed message M_s, formed from the plaintext message data M being cryptographically processed at the sender with multi-prime (k>2) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, $p_1, p_2, \ldots p_k$, is decipherable by the decoding at the recipient with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q.

38. (Previously Presented) The method according to claim 20, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to at composite number computed as the product of 2 prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

39. (Previously Presented) The method according to claim 22, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

40. (Previously Presented) A cryptography method for local storage of data by a private key owner,

comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} (\mathrm{mod}((p_1-1) \cdot (p_2-1) \cdots (p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers that are factors of n, where only the private key owner knows the factors of n; and

encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form $C \equiv M^e \pmod n$, wherein $0 \leq M \leq n-1$, whereby the ciphertext data C is decipherable only by the private key owner having available to it the factors of n.

41. (Previously Presented) The cryptography method in accordance with claim 40, further comprising the step of:

decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d \pmod n$.

42. (Previously Presented) A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to communicate with the plurality of stations via the communications medium sending a receiving messages cryptographically processed with an RSA public key encryption, the host system including

at least one cryptosystem configured for

developing k distinct random prime numbers, $p_1, p_2, \ldots, p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to a public key portion e that is associated with the host system,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship of the public key portion e in the form of $d \equiv e^{-1} \pmod{(p_1-1)\cdot(p_2-1)\cdots(p_k-1)}$,

in response to an encoding request from the host system, encoding a plaintext message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

in response to a decoding request from the host system, decoding a ciphertext message data C' communicated via the host producing therefrom a plaintext message data M' using a relationship of the form $M' \equiv C'^d \pmod{n}$.

43. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem communicatively coupled to and receiving from the bus encoding and decoding requests, the cryptosystem being configured for

providing a public key portion e,

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to the public key portion e,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} \pmod{(p_1-1)\cdot(p_2-1)\cdots(p_k-1)}$,

in response to an encoding request from the bus, encoding a plaintext form of a first message M to produce C, a ciphertext form of the first message, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$, and

in response to an decoding request from the host system, decoding C', a ciphertext form of a second message, to produce M', a plaintext form of the second message, using a relationship of the form $M' \equiv C'_d \pmod{n}$, the first and second messages being distinct or one and the same.

44. (Previously Presented) The system of claim 42, wherein the at least one cryptosystem includes

a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

45. (Previously Presented) The system of claim 42, wherein the at least one cryptosystem includes

a processor,

a data-address bus,

a memory coupled to the processor via the data-address bus,

a data encryption standard (DES) unit coupled the memory and the processor via the data-address bus,

a plurality of exponentiator elements coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. (Previously Presented) The system of claim 45, wherein the memory and each of the plurality of exponeniator elements has its own DES unit that cryptographically processes message data received/returned from/to the processor.

47. (Previously Presented) The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor, including secure, insecure and exponentiator elements address spaces, and wherein the DES unit is configured to recognize the secure and exponentiator elements address spaces and to automatically encode message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when the

processor is accessing the insecure memory address spaces, the DES unit being further configured to decode endoded message data received from the memory before it is provided to the processor.

48. (Previously Presented) The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

49. (Previously Presented) The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors $p_1, p_2, \ldots p_k$.

50. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the

cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding request

providing a plaintext message M to be encoded,

obtaining a public key that includes an exponent e and a modulus n, a

representation of the modulus n existing in the memory in the form of

its k distinct random prime number factors $p_1, p_2, \ldots p_k$, wherein $k>3$,

constructing subtasks, one subtask for each of the *k* factors, to be executed by the exponentiator elements for producing respective ones of the subtask values, $C_1, C_2, \ldots C_k$, and

forming a ciphertext message *C* from the subtask values $C_1, C_2, \ldots C_k$,

wherein the ciphertext message C is decipherable using a private key that includes the modulus *n* and an exponent *d* which is a function of *e*.

51. (Previously Presented) The system of claim 50, wherein each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\bmod p_i)$, where $M_i \equiv (\bmod p_i)$, and $e_i \equiv e(\bmod p_i-1)$, and where $i=1, 2, \ldots k$.

52. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding/decoding request provided with a plaintext/ciphertext message *M/C* to be encoded/decoded and with or without a public/private key that includes an exponenet *e/d* and a modulus *n* representation of which exists in the memory in the form of its *k* distinct random prime number $p_1, p_2, \ldots p_k$, where $k \geq 3$,

obtaining the public/private key from the memory if the encoding/decoding request is provided without the public/private key,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $M_1, M_2, \ldots M_k / C_1, C_2, \ldots C_k$, and

forming the ciphertext/plaintext message *C/M* from the subtask values $C_1, C_2, \ldots C_k / M_1, M_2, \ldots M_k$.

53. (Previously Presented) The system of claim 52 wherein when produced each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\mathrm{mod}\, p_i)$, where $C_1 \equiv C\ (\mathrm{mod}\ p_i)$, and $e_i \equiv e\ (\mathrm{mod}\ p_i - 1)$, and where $i = 1, 2, \ldots k$.

54. (Previously Presented) The system of claim 52 wherein when produced each one of the subtasks $M_1, M_2, \ldots M_k$ is developed using a relationship of the form $M_i \equiv C_i^{d_i} (\mathrm{mod}\, p_i)$, where $M_i \equiv M\ (\mathrm{mod}\ p_i)$, and $d_i \equiv d (\mathrm{mod}\ p_i - 1)$, and where $i = 1, 2, \ldots k$.

55. (Previously Presented) The system of claim 54, wherein the private key exponent *d* relates to the public key exponent *e* vai $d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$.

56. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion *e*;

means for developing k distinct random prime number $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion of d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\bmod((p_1 - 1)\cdot(p_2 - 1)\cdots(p_k - 1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers;

means for receiving a ciphertext message data C; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

57. (Previously Presented) The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

58. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime number $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is releatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1}(\bmod((p_1 - 1)\cdot(p_2 - 1)\cdots(p_k - 1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers; and

means for encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \le M \le n-1$, the signed message M_s being decipherable using the public key portion e.

59. (Previously Presented) The system of claim 58 further comprising the step of:

means for decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

60. (Previously Presented) The system of claim 57, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

61. (Previously Presented) The system of claim 59, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

REMARKS

This paper is filed in response to the U.S.P.T.O. communication dated April 8, 2005.

STATUS OF THE CLAIMS

As of the date of this Amendment, claims 1-6, 9-12, and 14-61 remain pending.

In response to the communication of April 8, 2005, Applicants hereby submit a complete set of the pending claims in the present application marked in accordance with 37 C.F.R. § 1.173.

The communication mailed April 8, 2005 indicates that Applicant has been given numerous attempts to correct the non-responsive Amendment of February 7, 2005 and any further non-responsiveness will be considered as a non-bona fide reply.

Applicants apologize for Applicant's previous attempts on March 18, 2005, and March 25, 2005, to properly mark the presently claims. However, Applicants respectfully asserts that each of those responses was submitted in a bona fide attempt to satisfy specific requests by Examiner Seal and Examiner Laufer. Applicants respectfully assert that part of the confusion resulting in the responses of March 18 and March 25, 2005, were the result of conflicting requests by the above two Examiners.

Applicants respectfully submit the enclosed bona fide response, in order to satisfy the requirements set forth by Examiner Smithers.

I. STATUS OF THE CLAIMS

As of the date of this Amendment, claims 1-6 and 9-12, 14-61 remain pending. Claims 4 and 35 have been amended. Claims 1, 3-5, 9, 11, 14, 16, 18, 20, 22, 40, 42-43, 50, 52, 56, and 58 are independent claims.

PART 1 - SUMMARY OF THE ISSUES IN THE PRESENT APPLICATION

I. Introduction

Applicants assert that many of the primary issues (i.e., establishing that publications are actually prior art references, motivation for combining prior art references, etc.) raised in Applicant's previous response of October 14, 2003, which thoroughly rebutted all of the Examiner's objections and rejections, have nöt been addressed by the Examiner. Applicants further assert that until such time as the Examiner addresses the primary issues raised by Applicants, all of the Examiner's additional, secondary issues raised in the outstanding office action of October 7, 2004, are not ripe for argument.

In an effort to focus prosecution on these key, primary issues, Applicants' offer the following summary. This Summary is followed by Part 2, which specifically addresses the additional, secondary issues in the outstanding office action of October 7, 2004.

II. General Summary of the Present Invention

In a broad, general sense, example embodiments of the present invention are directed to methods and systems of communicating messages cryptographically, which use three or more random and distinct prime numbers. Claims directed to such example methods include presently pending independent claims 1, 3, 14, 16, 18, 20, 22, and 40. Claims directed to such example systems include presently pending independent claims 4, 5, 9, 11, 42, 43, 50, 52, 56, and 58.

Other example embodiments are directed to methods and systems of communicating messages cryptographically, which develop subtask values corresponding to the message in parallel. Claims directed to such example systems include presently pending dependent claims 44 and 45.

III. Support in the Original Collins et al. Patent for the General Invention

Applicants respectfully submit that column 3, line 27-29 of the original Collins et al. patent recite that it is an object of the present invention to provide a system and method for utilizing "multiple (more than two) distinct prime number components to create n." Further, column 3, lines 40-41 of the original Collins et al. patent recite that "n is developed from three or more distinct prime numbers; i.e., $n = p_1 \cdot p_2 \cdot \ldots p_k$, where k is an integer greater than two." Column 5, lines 31-32 recite an example assuming three or more random, large, distinct primes, p_1, p_2, $\ldots p_k$. Column 5, lines 66-67 recite an example assuming three distinct primes, p_1, p_2, and p_3. The original abstract also recites "three or more distinct primes.". Accordingly, Applicants respectfully submit that the original Collins et al. patent at least supports claims directed to more than two distinct prime numbers, three distinct prime numbers, three or more distinct prime numbers, and three or more random and distinct prime numbers. Applicants fail to see how the Examiner could conclude otherwise.

IV. Establishing Various, Alleged Prior Art References are In Fact Prior Art

A. U.S. Patent 5,974,151 to Slavin

The Examiner has applied U.S. Patent 5,974,151 to Slavin against several claims of the present application under 35 U.S.C. § 102(a). 35 U.S.C. § 102(a) states:

A person shall be entitled to a patent unless -

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent,...

A cursory inspection of Slavin reveals Slavin was published on October 26, 1999, almost three (3) years **after** the present application was filed (on January 16, 1997) and almost eleven (11) months **after** the Collins et al. patent was **granted** (on December 8, 1998). Applicants are at loss to explain how the Examiner could conclude Slavin is 35 U.S.C. § 102(a) prior art against the present application.

B. "RSA Moduli Should Have 3 Prime Factors" to Captain Nemo

The Examiner has again applied "RSA Moduli Should Have 3 Prime Factors" to Captain Nemo against several claims of the present application under 35 U.S.C. § 103(a). While the exact basis for this rejection is unclear, Applicants assume the basis is under 35 U.S.C. § 102(b). 35 U.S.C. § 102(b) states:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States, ...

Applicants will not further debate the merits of the teachings of Nemo, until the Examiner can establish that Nemo is, in fact, prior art against the present application. Applicants continue to assert that the Examiner has not established that Nemo is, in fact, a publication. The date on which the **public actually gained access** to Nemo is the relevant date.

On its face, Nemo states that it was published in "Scientific Bulgarian" magazine in August 1996. Applicants have checked the existence of "Scientific Bulgarian" magazine and have concluded that a paper form of an "August 1996" issue (or any other paper issue containing Nemo) was never produced or made available to the public. If the Examiner can establish otherwise, he is invited to do so. If not, he should withdraw all rejections relying on Nemo.

Applicants have further checked the Internet for any credible evidence of the presence of an electronic copy of Nemo available to the public via the Internet prior to the filing date of the present application and have concluded that Nemo was also not available in electronic form. If the Examiner can establish otherwise, he is invited to do so. If not, he should withdraw all rejections relying on Nemo.

Finally, Applicants conducted a quick and rudimentary search of the U.S.P.T.O's patent database (at www.uspto.gov) from 1976 to the present and have discovered that **not one issued U.S. patent** in that time period lists Nemo or any other article from any other issue of "Scientific Bulgarian" magazine as a prior art publication.

V. The Teachings of Various Prior Art References With Respect to "Three or More Random and Distinct Prime Numbers"

A. General

The Examiner has asserted that several prior art references teach three or more random and distinct prime numbers without ever specifically setting forth such a teaching. Applicants find this rationale particularly confusing when contrasted with the Examiner's position that the present application, which specifically refers to "three or more random and distinct prime numbers" at col. 5, lines 31-32, **does not** teach "three or more random and

distinct prime numbers". Applicants will address each of these references individually below.

B. U.S. Patent 4,405,829 to Rivest et al (RSA)

RSA teaches two or more distinct primes. Nowhere does RSA even mention "random", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert RSA fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

C. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems" by Rivest et al. (Rivest)

Rivest teaches two random primes. Nowhere does Rivest even mention "distinct", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert Rivest fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

D. The Art of Computer Programming by Knuth (Knuth)

Knuth teaches nothing about prime numbers. Nowhere does Knuth even mention "random", let alone "distinct", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert Knuth fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

E. "Using four-prime RSA in which some bits are Specified" by Vanstone and Zuccherato (Vanstone)

Vanstone teaches four prime numbers. Nowhere does Vanstone even mention "random", let alone "distinct", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert Vanstone fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

F. "A Public-Key Cryptosystem Suitable for Digital Multisignatures" by Itakura and Nakamura (Itakura)

Itakura teaches three prime numbers. Nowhere does Itakura even mention "random", let alone "distinct", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert Itakura fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

VI. Motivation for Combining Various Prior Art References

A. General

It is apparent that in the above section, applicants have taken each valid prior art reference separately and compared it to a broad characterization of the present invention, a broad characterization which is present in each and every independent claim. A proper analysis does not conclude with a discussion of the teachings of the prior art references individually, especially in a § 103 rejection. Of course, to establish a § 103 rejection, it is impermissible for an Examiner to pick and choose various teachings of the prior art references, in order to piece together the invention recited in the claims to be rejected.

In Applicants' prior response of October 14, 2003, Applicants challenged the Examiner's motivation for combining RSA, Rivest, and Knuth. In the outstanding office

action of October 7, 2004, which includes 68 paragraphs over 25 pages (and raises scores of secondary issues, all tangential to the primary issues laid out above), the Examiner devotes a total of one sentence to motivation. The sentence in question can be found on page 23, at the end of paragraph 67, where the Examiner, apparently trying to establish motivation for combining RSA and Rivest, states:

> "The motivation for distinct randomly choosen (sic) distinct multiprime comes from the same authors and thus is not pieced together."

Applicants are aware of no valid, current, U.S. patent decision which has held that two publications by one author or inventor or one set of authors or inventors, is per se, combinable under 35 U.S.C. § 103(a). In fact, in at least *In re Kotzab*, 217 F.3d 1365, 55 USPQ2d 1313 (Fed. Cir. 2000), the CAFC held that even separate embodiments of the **same patent** cannot be combined absent some motivation to do so.[1]

B. RSA and Rivest

As set forth above, the mere fact that two publications are from the same author(s) or inventor(s) is not sufficient motivation to combine them. Accordingly, Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA and Rivest in order to piece together the invention recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

C. RSA and Knuth

[1] The Examiner's argument in paragraph 23 is also contrary to the holding of *Kotzab*.

Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA and Knuth in order to piece together the invention recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

D. Rivest and Knuth

Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Rivest and Knuth in order to piece together the invention recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

E. Itakura and Rivest

Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Itakura and Rivest in order to piece together the invention recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

PART 2 - OTHER ISSUES RAISED IN THE OUTSTANDING OFFICE ACTION OF OCTOBER 7, 2004

I. OBJECTION TO THE SPECIFICATION – NEW MATTER

Sections 1-6 and 61-66 of the outstanding office action of October 7, 2003, indicate that Applicants' previous amendment of October 14, 2003 has been objected to under 35 U.S.C. § 132 as having allegedly introduced new matter into the specification.

In Sections 2 and 63, the Examiner objects to the replacement of the term "using" with the term "extending". Applicants assert that the conventional RSA scheme uses two primes, whereas the present invention uses three or more. In this context, Applicants believe that the present invention "extends" the number of primes from two to three or more. As a result, Applicants believe that the present invention "extends" the RSA scheme. Accordingly, reconsideration and withdrawal of the objection is respectfully requested.

In Sections 3 and 64, the Examiner asserts that the change that "three or more random large, distinct primed numbers are developed and checked to ensure that each (p_i-1) is relatively prime to e" is new matter.

Applicants direct the Examiner's attention to originally filed independent claim 1, filed on January 16, 1997 which recites e is a number relatively prime to $(p_1-1) \cdot (p_2-1) \cdot \ldots (p_k-1)$. Accordingly, Applicants respectfully submit that the change to column 5, lines 31-33, merely brings the specification into compliance with original claim 1. Further, Applicants respectfully submit that one of ordinary skill in the art would recognize that the equation recited at column 5, line 39 would not work if three or more random large distinct prime numbers were not relatively prime to e. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In Sections 4 and 62, the Examiner asserts that the amendment to column 5, line 52, to add a digital signature, is not supported. However, Applicants have been unable to locate the addition of a "digital signature" in Applicants previous response. Clarification of this rejection is requested.

In Sections 5 and 64, the Examiner asserts that the amendment to the specification to column 6, line 24 to change "$i \geq 2$" to "$2 \leq i \leq k$ where k is the number of primes in n" constitutes new matter.

Applicants respectfully submit that this change merely more accurately recites the teachings of the present invention. As set forth clearly throughout the specification, there are no prime numbers beyond p_k; accordingly, it makes absolutely no sense to indicate prime numbers greater than equal to 2, but unbounded by the number of prime numbers k. Accordingly, Applicants respectfully submit that this is not new matter, but merely a reflection of the upper bound of the number of k primes, which the change of which, Applicants believe more accurately represents the present invention. However, although less accurate, Applicants are willing to leave this portion of the specification as "$i \geq 2$".

In Section 6, with regard to column 6, line 65, the Examiner asserts that the change from "the decrypted message M can be obtained" to "the ciphertext C can be obtained" is new matter. The Examiner further asserts that in the first version, summation is required, wherein the second version iteration is required.

In response to this objection, Applicants respectfully submit that there are at least two know solutions for the Chinese Remainder Theorem. The first, proposed by Gauss, is a summation technique, and therefore not recursive. The second, proposed by Garner, is a recursive technique. Applicants respectfully submit that the original patent describes Garner's technique beginning at column 6, line 1 and Gauss' technique, beginning at column 7, line 1. Since the present application supports both recursive and non-recursive solutions, Applicants assert that the Amendment to column 6, line 65 does not constitute new matter.

II. CLAIM OBJECTIONS

In Sections 7 and 8, the Examiner points out minor informalities in the previous amendments to claims 4 and 35. Applicants have amended claims 4 and 35 to correct these minor informalities.

III. CLAIM REJECTIONS UNDER 35 U.S.C. § 112

A. 35 U.S.C. § 112, FIRST PARAGRAPH

In Section 10, claim 1 is rejected under 35 U.S.C. § 112, first paragraph but no specific rejection is set forth. Applicants assume this rejection is related to the objection to the specification under 35 U.S.C. § 132 and therefore traversed for the reasons set forth above.

In Sections 11 and 12, the Examiner asserts that claims 1-2, 18-19, 32-33, 37, 42-49, and 56-61 are rejected under 35 U.S.C. § 112, first paragraph, because the patent as originally filed does not disclose $k \geq 3$. Applicants respectfully submit that column 3, line 27-29 of the original Collins et al. patent recite that it is an object of the present invention is to provide a system and method for utilizing "multiple (more than two) distinct prime number components to create n." Further, column 3, lines 40-41 of the original Collins et al. patent recite that "n is developed from three or more distinct prime numbers; i.e., $n = p_1 \cdot p_2 \cdot \ldots p_k$, where k is an integer greater than two." Finally, column 5, lines 66-67 recite an example assuming three distinct primes, p_1, p_2, and p_3. Accordingly, Applicants respectfully submit that an amendment reciting k is an integer greater than two is supported by multiple passages in the original Collins et al. patent.

In Sections 13-15, the Examiner asserts that claims 1-61 are rejected under 35 U.S.C. § 112, first paragraph, objecting to the term "random". The Examiner correctly points out that the term random is utilized in the original patent at column 5, line 31 and is therefore supported by the original patent. Applicants assert that this disclosure supports the claims as amended.

In Applicants previous Response, Applicants asserted that "the randomness and distinctness attributes of the k prime numbers will materially improve the security in any cryptographic system with RSA public key encryption".

With respect to this statement, the Examiner asserts that if this were the intent of the original patent, the original patent does not support this view. Applicants respectfully submit that the above statement is an advantage of the present invention. Advantages of the present invention need not be provided in the specification In re Chu, 36 U.S.P.Q.2d 1089 (Fed.Cir. 1995). Accordingly, Applicants respectfully submit that claims 1-61 are supported by the original specification, because random is provided in the original patent, and any purported advantage of the randomness need not be present in the original patent.

B. 35 U.S.C. 112, SECOND PARAGRAPH

In Section 18, the Examiner objects to amended claim 9, specifically the word "means" is not followed by a function. Applicants have reviewed claim 9 and are unsure of the Examiner's rejection, in particular, each means clause of claim 9 appears to recite a function.

IV. CLAIM REJECTIONS UNDER 35 U.S.C. § 103

In sections 19-49 and 67 of the Office Action, claims 1-7, 9-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 4,405,829 to Rivest et al., (RSA), and further in view of Rivest et al. "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Communications of the ACM, 21(2) February 1978, (Rivest) and further in view of Knuth, The Art of Computer Programming Vol. 2, page 179 (Knuth).

This rejection is respectfully traversed for the reasons set forth above in Part 1, Sections V-A through V-D and Sections VI-A through VI-D, and for the reasons set forth in Applicants' previous response of October 14, 2003.

In Sections 53 and 60, claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo (RSA Moduli Should Have 3 Prime Factors) (Nemo), and further in view of Rivest.

This rejection is respectfully traversed for the reasons set forth above in Part 1, Section IV-B, Section V-A, and Section VI-A, and for the reasons set forth in Applicants' previous response of October 14, 2003.

In Section 56, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Itakura and Nakamura, A Public-Key Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No. 71, October (Itakura), and further in view of Rivest.

This rejection is respectfully traversed for the reasons set forth above in Part 1, Sections V-A and V-F and Sections VI-A and VI-E, and for the reasons set forth in Applicants' previous response of October 14, 2003.

V. CLAIM REJECTION UNDER 35 U.S.C. § 102

In Sections 50-52 and 68, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 are rejected under 35 U.S.C. § 102(b) as being anticipated by Vanstone and Zuccherato, "Using four-prime RSA in which some bits are Specified", Electronic Letters, 30(25), 16 August 1994, (Vanstone).

This rejection is respectfully traversed for the reasons set forth above in Part 1, Sections V-A and V-E, and for the reasons set forth in Applicants' previous response of October 14, 2003.

In Sections 58, claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 102(a) as being anticipated by Slavin.

This rejection is respectfully traversed for the reasons set forth above in Part 1, Section IV-A.

CONCLUSION

In view of the above-amendments and remarks, reconsideration of the objections and rejections in allowance in each of claims 1-6, 9-12, 14-61 in connection with the present application is earnestly solicited.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By ______________________________

John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/pjd

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the Supplemental Amendment filed concurrently herewith, was served via first class mail, this 9th day of May, 2005 to:

Patent Administrator
Testa, Hurwitz & Thibeault, LLP
125 High Street
Boston, Massachusetts 02110

John A. Castellano, Esquire